Garside groups and Yang-Baxter equation

Fabienne Chouraqui

Abstract

We establish a one-to-one correspondence between a class of Garside groups admitting a certain presentation and the structure groups of non-degenerate, involutive and braided set-theoretical solutions of the quantum Yang-Baxter equation. We also characterize indecomposable solutions in terms of Δ-pure Garside groups.

1 Introduction

The quantum Yang-Baxter equation is an equation in the field of mathematical physics and it lies in the foundation of the theory of quantum groups. Let $R : V \otimes V \to V \otimes V$ be a linear operator, where V is a vector space. The quantum Yang-Baxter equation is the equality $R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}$ of linear transformations on $V \otimes V \otimes V$, where R^{ij} means R acting on the ith and jth components.

A set-theoretical solution of this equation is a solution for which V is a vector space spanned by a set X and R is the linear operator induced by a mapping $X \times X \to X \times X$. The study of these was suggested by Drinfeld [10]. Etingof, Soloviev and Schedler study set-theoretical solutions (X, S) of the quantum Yang-Baxter equation that are non-degenerate, involutive and braided [11]. To each such solution, they associate a group called the structure group and they show that this group satisfies some properties. They also give a classification of such solutions (X, S) up to isomorphism, when the cardinality of X is up to eight. As an example, there are 23 solutions for X with four elements, 595 solutions for X with six elements and 34528 solutions for X with eight elements. In this paper, we establish a one-to-one correspondence between non-degenerate, involutive and braided set-theoretical solutions of the quantum Yang-Baxter equation (up to isomorphism) and Garside presentations which satisfy some additional conditions up to t-isomorphism (a notion that will be defined below). The main result is as follows.

Theorem 1. (i) *Let X be a finite set, and (X,S) be a non-degenerate, involutive and braided set-theoretical solution of the quantum Yang-Baxter equation. Then the structure group of (X,S) is a Garside group.*
(ii) *Conversely, assume that* $\mathrm{Mon}\langle X \mid R\rangle$ *is a Garside monoid such that:*
- the cardinality of R is $n(n-1)/2$, where n is the cardinality of X and each side of a relation in R has length 2 and
- if the word x_ix_j appears in R, then it appears only once.
Then there exists a function $S : X \times X \to X \times X$ such that (X,S) is a non-degenerate, involutive and braided set-theoretical solution and $\mathrm{Gp}\langle X \mid R\rangle$ *is its structure group.*

The main idea of the proof is to express the right and left complement on the generators in terms of the functions that define (X,S). Moreover, we prove that the structure group of a set-theoretical solution satisfies some specific constraints. Picantin defines the notion of Δ-pure Garside group in [16] and he shows that the center of a Δ-pure Garside group is a cyclic subgroup that is generated by some exponent of its Garside element.

Theorem 2. *Let X be a finite set, and (X,S) be a non-degenerate, involutive and braided set-theoretical solution of the quantum Yang-Baxter equation. Let G be the structure group of (X,S) and M the monoid with the same presentation. Then*
(i) *The right least common multiple of the elements in X is a Garside element in M.*
(ii) *The (co)homological dimension of G is equal to the cardinality of X.*
(iii) *The group G is Δ-pure Garside if and only if (X,S) is indecomposable.*

Point (i) above means that G is Garside in the restricted sense of [9]. Let us observe that, independently, Gateva-Ivanova and Van den Bergh define in [14] monoids and groups of left and right I-type and they show that they yield solutions to the quantum Yang-Baxter equation. They show also that a monoid of left I-type is cancellative and has a group of fractions that is torsion-free and Abelian-by-finite. Jespers and Okninski extend their results in [15], and establish a correspondence between groups of I-type and the structure group of a non-degenerate, involutive and braided set-theoretical solution. Using our result, this makes a correspondence between groups of I-type and the class of Garside groups studied in this paper. They also remark that the defining presentation of a monoid of I-type satisfies the right cube condition, as defined by Dehornoy in [7, Prop.4.4]. So, the necessity of being Garside can be derived from the combination of the results from [15, 14]. Our methods in this paper are different as we use the tools of

reversing and complement developed in the theory of Garside monoids and groups and our techniques of proof are uniform throughout the paper. It can be observed that our results imply some earlier results by Gateva-Ivanova. Indeed, she shows in [13] that the monoid corresponding to a special case of non-degenerate, involutive and braided set-theoretical solution (square-free) has a structure of distributive lattice with respect to left and right divisibility and that the left least common multiple of the generators is equal to their right least common multiple and she calls this element the principal monomial.

The paper is organized as follows. In section 2, we give some preliminaries on Garside monoids. In section 3, we give the definition of the structure group of a non-degenerate, involutive and braided set-theoretical solution and we show that it is Garside, using the criteria developed by Dehornoy in [4]. This implies that this group is torsion-free from [6] and biautomatic from [4]. In section 4, we show that the right least common multiple of the generators is a Garside element and that the (co)homological dimension of the structure group of a non-degenerate, involutive and braided set-theoretical solution is equal to the cardinality of X. In section 5, we give the definition of a Δ-pure Garside group and we show that the structure group of (X, S) is Δ-pure Garside if and only if (X, S) is indecomposable. In section 6, we establish a converse to the results of section 3, namely that a Garside monoid satisfying some additional conditions defines a non-degenerate, involutive and braided set-theoretical solution of the quantum Yang-Baxter equation. Finally, in section 7, we address the case of non-involutive solutions. There, we consider the special case of permutation solutions that are not involutive and we show that their structure group is Garside. We could not extend this result to general solutions, although we conjecture this should be true. At the end of the section, we give the form of a Garside element in the case of permutation solutions.

Acknowledgment. This work is a part of the author's PhD research, done at the Technion under the supervision of Professor Arye Juhasz. I am very grateful to Professor Arye Juhasz, for his patience, his encouragement and his many helpful remarks. I am also grateful to Professor Patrick Dehornoy for his comments on this paper.

2 Garside monoids and groups

All the definitions and results in this section are from [4] and [5]. In this paper, if the element x of M is in the equivalence class of the word w, we say that w *represents* x.

2.1 Garside monoids

Let M be a monoid and let x, y, z be elements in M. The element x is *a left divisor* of z if there is an element t such that $z = xt$ in M and z is *a right least common multiple (right lcm)* of x and y if x and y are left divisors of z and additionally if there is an element w such that x and y are left divisors of w, then z is left divisor of w. We denote it by $z = x \vee y$. *The complement at right of* y *on* x is defined to be an element $c \in M$ such that $x \vee y = xc$, whenever $x \vee y$ exists. We denote it by $c = x \setminus y$ and by definition, $x \vee y = x(x \setminus y)$. Dehornoy shows that if M is left cancellative and 1 is the unique invertible element in M, then the right lcm and the right complement of two elements are unique, whenever they exist [4]. We refer the reader to [5, 4] for the definitions of the left lcm and the left and right gcd of two elements. An element x in M is *an atom* if $x \neq 1$ and $x = yz$ implies $y = 1$ or $z = 1$. The *norm* $\parallel x \parallel$ of x is defined to be the supremum of the lengths of the decompositions of x as a product of atoms. The monoid M is *atomic* if M is generated by its atoms and for every x in M the norm of x is finite. It holds that if all the relations in M are length preserving, then M is atomic, since each element x of M has a finite norm as all the words which represent x have the same length.

A monoid M is *Gaussian* if M is atomic, left and right cancellative, and if any two elements in M have a left and right gcd and lcm. If Δ is an element in M, then Δ is a *Garside element* if the left divisors of Δ are the same as the right divisors, there is a finite number of them and they generate M. A monoid M is *Garside* if M is Gaussian and it contains a Garside element. A group G is a *Gaussian group* (respectively a *Garside group*) if there exists a Gaussian monoid M (respectively a Garside monoid) such that G is the fraction group of M. A Gaussian monoid satisfies both left and right Ore's conditions, so it embeds in its group of fractions (see [3]). As an example, braid groups and Artin groups of finite type [12], torus knot groups [18] are Garside groups.

Definition 2.1. [4, Defn.1.6] Let M be a monoid. M satisfies:
- (C_0) if 1 is the unique invertible element in M.
- (C_1) if M is left cancellative.

- $(\tilde{C_1})$ if M is right cancellative.
- (C_2) if any two elements in M with a right common multiple admit a right lcm.
- (C_3) if M has a finite generating set P closed under $\backslash$, i.e if $x, y \in P$ then $x \setminus y \in P$.

Theorem 2.2. *[4, Prop. 2.1] A monoid M is a Garside monoid if and only if M satisfies the conditions (C_0), (C_1), $(\tilde{C_1})$, (C_2), and (C_3).*

2.2 Recognizing Garside monoids

Let X be an alphabet and denote by ϵ the empty word in X^*. Let f be a partial function of $X \times X$ into X^*, f is a *complement* on X if $f(x, x) = \epsilon$ holds for every x in X, and $f(y, x)$ exists whenever $f(x, y)$ does. The congruence on X^* generated by the pairs $(xf(x, y), yf(y, x))$ with (x, y) in the domain of f is denoted by "$\equiv^+$". The monoid *associated with* f is $X^*/\equiv^+$ or in other words the monoid $\mathrm{Mon}\langle X \mid xf(x, y) = yf(y, x)\rangle$ (with (x, y) in the domain of f). The complement mapping considered so far is defined on letters only. Its extension on words is called *word reversing* (see [5]).

Example 2.3. Let M be the monoid generated by $X = \{x_1, x_2, x_3, x_4, x_5\}$ and defined by the following 10 relations.

$$x_1^2 = x_2^2 \quad x_2x_5 = x_5x_2 \quad x_1x_2 = x_3x_4 \quad x_1x_5 = x_5x_1 \quad x_1x_3 = x_4x_2$$
$$x_3^2 = x_4^2 \quad x_2x_4 = x_3x_1 \quad x_3x_5 = x_5x_3 \quad x_2x_1 = x_4x_3 \quad x_4x_5 = x_5x_4$$

Then the complement f is defined totally on $X \times X$ and the monoid associated to f, $X^*/\equiv^+$, is M. As an example, $f(x_1, x_2) = x_1$ and $f(x_2, x_1) = x_2$ are obtained from the relation $x_1^2 = x_2^2$, since it holds that $f(x_1, x_2) = x_1 \backslash x_2$.

Let f be a complement on X. For $u, v, w \in X^*$, f is *coherent* at (u, v, w) if either $((u \setminus v) \setminus (u \setminus w)) \setminus ((v \setminus u) \setminus (v \setminus w)) \equiv^+ \epsilon$ holds, or neither of the words $((u \backslash v) \backslash (u \backslash w)), ((v \backslash u) \backslash (v \backslash w))$ exists. The complement f *is coherent* if it is coherent at every triple (u, v, w) with $u, v, w \in X^*$. Dehornoy shows that if the monoid is atomic then it is enough to show the coherence of f on its set of atoms. Moreover, he shows that if M is a monoid associated with a coherent complement, then M satisfies C_1 and C_2 (see [5, p.55]).

Proposition 2.4. *[4, Prop.6.1] Let M be a monoid associated with a complement f and assume that M is atomic. Then f is coherent if and only if f is coherent on X.*

Example 2.5. In example 2.3, we check if $((x_1 \setminus x_2) \setminus (x_1 \setminus x_3)) \setminus ((x_2 \setminus x_1) \setminus (x_2 \setminus x_3)) = \epsilon$ holds in M. We have $x_1 \setminus x_2 = x_1$ and $x_1 \setminus x_3 = x_2$, so $(x_1 \backslash x_2) \backslash (x_1 \backslash x_3) = x_1 \backslash x_2 = x_1$. Additionally, $x_2 \backslash x_1 = x_2$ and $x_2 \backslash x_3 = x_4$,

so $(x_2 \setminus x_1) \setminus (x_2 \setminus x_3) = x_2 \setminus x_4 = x_1$. At last, $((x_1 \setminus x_2) \setminus (x_1 \setminus x_3)) \setminus ((x_2 \setminus x_1) \setminus (x_2 \setminus x_3)) = x_1 \setminus x_1 = \epsilon$.

3 Structure groups are Garside

3.1 The structure group of a set-theoretical solution

All the definitions and results in this subsection are from [11].

A set-theoretical solution of the quantum Yang-Baxter equation is a pair (X, S), where X is a non-empty set and $S : X^2 \to X^2$ is a bijection. Let S_1 and S_2 denote the components of S, that is $S(x, y) = (S_1(x, y), S_2(x, y))$. A pair (X, S) is *nondegenerate* if the maps $X \to X$ defined by $x \mapsto S_2(x, y)$ and $x \mapsto S_1(z, x)$ are bijections for any fixed $y, z \in X$. A pair (X, S) is *braided* if S satisfies the braid relation $S^{12}S^{23}S^{12} = S^{23}S^{12}S^{23}$, where the map $S^{ii+1} : X^n \to X^n$ is defined by $S^{ii+1} = id_{X^{i-1}} \times S \times id_{X^{n-i-1}}$, $i < n$. A pair (X, S) is *involutive* if $S^2 = id_{X^2}$, that is $S^2(x, y) = (x, y)$ for all $x, y \in X$.
Let $\alpha : X \times X \to X \times X$ be the permutation map, that is $\alpha(x, y) = (y, x)$, and let $R = \alpha \circ S$. The map R is called the *$R-$matrix corresponding to S*. Etingof, Soloviev and Schedler show in [11], that (X, S) is a braided set if and only if R satisfies the quantum Yang-Baxter equation $R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}$, where R^{ij} means acting on the ith and jth components and that (X, S) is a symmetric set if and only if in addition R satisfies the unitary condition $R^{21}R = 1$. They define the *structure group G of* (X, S) to be the group generated by the elements of X and with defining relations $xy = tz$ when $S(x, y) = (t, z)$. They show that if (X, S) is non-degenerate and braided then the assignment $x \to f_x$ is a right action of G on X.

We use the notation of [11], that is if X is a finite set, then S is defined by $S(x, y) = (g_x(y), f_y(x))$, x, y in X. Here, if $X = \{x_1, ..., x_n\}$ is a finite set and $y = x_i$ for some $1 \leq i \leq n$, then we write f_i, g_i instead of f_y, g_y and $S(i, j) = (g_i(j), f_j(i))$. The following claim from [11] translates the properties of a solution (X, S) in terms of the functions f_i, g_i and it will be very useful in this paper.

Claim 3.1. *(i) S is non-degenerate $\Leftrightarrow$ f_i, g_i are bijective,* $1 \leq i \leq n$.
(ii) S is involutive $\Leftrightarrow$ $g_{g_i(j)}f_j(i) = i$ and $f_{f_j(i)}g_i(j) = j$, $1 \leq i, j \leq n$.
(iii) S is braided $\Leftrightarrow$ $g_ig_j = g_{g_i(j)}g_{f_j(i)}$, $f_jf_i = f_{f_j(i)}f_{g_i(j)}$,
and $f_{g_{f_j(i)}(k)}g_i(j) = g_{f_{g_j(k)}(i)}f_k(j)$, $1 \leq i, j, k \leq n$.

Example 3.2. Let$X = \{x_1, x_2, x_3, x_4, x_5\}$ and $S(i,j) = (g_i(j), f_j(i))$. Assume

$f_1 = g_1 = (1,2,3,4)(5) \quad f_2 = g_2 = (1,4,3,2)(5)$
$f_3 = g_3 = (1,2,3,4)(5) \quad f_4 = g_4 = (1,4,3,2)(5)$

Assume also that the functions f_5 and g_5 are the identity on X. Then a case by case analysis shows that (X,S) is a non-degenerate, involutive and braided solution. Its structure group is generated by X and defined by the 10 relations described in example 2.3.

3.2 Structure groups are Garside

In this subsection, we prove the following result.

Theorem 3.3. *The structure group G of a non-degenerate, braided and involutive set-theoretical solution of the quantum Yang-Baxter equation is a Garside group.*

In order to prove that the group G is a Garside group, we show that *the monoid M with the same presentation* is a Garside monoid. For that, we use the Garsidity criterion given in Theorem 2.2, that is we show that M satisfies the conditions (C_0) , (C_1) , (C_2), (C_3), and $(\tilde{C_1})$. We refer the reader to [14, Lemma 4.1] for the proof that M is right cancellative (M satisfies $(\tilde{C_1})$). We first show that M satisfies the conditions (C_0). In order to do that, we describe the defining relations in M and as they are length-preserving, this implies that M is atomic.

Claim 3.4. *Assume (X,S) is non-degenerate. Let x_i and x_j be different elements in X. Then there is exactly one defining relation $x_ia = x_jb$, where a, b are in X. If in addition, (X,S) is involutive then a and b are different.*

For a proof of this result, see [14, Thm. 1.1]. Using the same arguments, if (X,S) is non-degenerate and involutive there are no relations of the form $ax_i = ax_j$, where $i \neq j$. We have the following direct result from claim 3.4.

Proposition 3.5. *Assume (X,S) is non-degenerate and involutive. Then the complement f is totally defined on $X \times X$, its range is X and the monoid associated to f is M. Moreover, M is atomic.*

Now, we show that M satisfies the conditions (C_1), (C_2) and (C_3). From Proposition 3.5, we have that there is a one-to-one correspondence between the complement f and the monoid M with the same presentation as the structure group, so we say that M is coherent (by abuse of notation). In order to show that the monoid M satisfies the conditions (C_1) and (C_2), we

show that M is coherent (see [5, p.55]). Since M is atomic, it is enough to check its coherence on X (from Proposition 2.4). We show that any triple of generators (a, b, c) satisfies the following equation: $(a \setminus b) \setminus (a \setminus c) = (b \setminus a) \setminus (b \setminus c)$, where the equality is in the free monoid X^*, since the range of f is X. In the following lemma, we establish a correspondence between the right complement of generators and the functions g_i that define (X, S).

Lemma 3.6. *Assume (X, S) is non-degenerate. Let x_i, x_j be different elements in X. Then $x_i \setminus x_j = g_i^{-1}(j)$.*

Proof. If $S(i, a) = (j, b)$, then $x_i \setminus x_j = a$. But by definition of S, we have that $S(i, a) = (g_i(a), f_a(i))$, so $g_i(a) = j$ which gives $a = g_i^{-1}(j)$. □

Lemma 3.7. *Assume (X, S) is non-degenerate and involutive. Let x_i, x_k be elements in X. Then $g_k^{-1}(i) = f_{g_i^{-1}(k)}(i)$*

Proof. Since S is involutive, we have from claim 3.1 that for every $x_i, x_j \in X$, $g_{g_i(j)} f_j(i) = i$. We replace in this formula j by $g_i^{-1}(k)$ for some $1 \leq k \leq n$, then we obtain $i = g_{g_i(g_i^{-1}(k))} f_{g_i^{-1}(k)}(i) = g_k f_{g_i^{-1}(k)}(i)$. So, we have $g_k^{-1}(i) = f_{g_i^{-1}(k)}(i)$. □

Proposition 3.8. *Assume (X, S) is non-degenerate, involutive and braided. Every triple (x_i, x_k, x_m) of generators satisfies the following equation: $(x_i \setminus x_k) \setminus (x_i \setminus x_m) = (x_k \setminus x_i) \setminus (x_k \setminus x_m)$. Furthermore, M is coherent and satisfies the conditions (C_1) and (C_2).*

Proof. If $x_i = x_k$ or $x_i = x_m$ or $x_k = x_m$, then the equality holds trivially. So, assume that (x_i, x_k, x_m) is a triple of different generators. This implies that $g_i^{-1}(k) \neq g_i^{-1}(m)$ and $g_k^{-1}(i) \neq g_k^{-1}(m)$, since the functions g_i are bijective. Using the formulas for all different $1 \leq i, k, m \leq n$ from lemma 3.6, we have: $(x_i \setminus x_k) \setminus (x_i \setminus x_m) = g^{-1}_{x_i \setminus x_k}(x_i \setminus x_m) = g^{-1}_{g_i^{-1}(k)} g_i^{-1}(m)$ and $(x_k \setminus x_i) \setminus (x_k \setminus x_m) = g^{-1}_{x_k \setminus x_i}(x_k \setminus x_m) = g^{-1}_{g_k^{-1}(i)} g_k^{-1}(m)$. We prove that $g^{-1}_{g_i^{-1}(k)} g_i^{-1}(m) = g^{-1}_{g_k^{-1}(i)} g_k^{-1}(m)$ by showing that $g_i g_{g_i^{-1}(k)} = g_k g_{g_k^{-1}(i)}$ for all $1 \leq i, k \leq n$. Since S is braided, we have from claim 3.1, that $g_i g_{g_i^{-1}(k)} = g_{g_i(g_i^{-1}(k))} g_{f_{g_i^{-1}(k)}(i)} = g_k g_{f_{g_i^{-1}(k)}(i)}$. But, from lemma 3.7, $f_{g_i^{-1}(k)}(i) = g_k^{-1}(i)$, so $g_i g_{g_i^{-1}(k)} = g_k g_{g_k^{-1}(i)}$. The monoid M is then coherent at X but since M is atomic, M is coherent. So, M satisfies the conditions (C_1) and (C_2). □

Now, using the fact that M satisfies (C_1) and (C_2), we show that it satisfies also (C_3).

Proposition 3.9. *Assume (X, S) is non-degenerate, involutive and braided. Then there is a finite generating set that is closed under $\setminus$, that is M satisfies the condition (C_3).*

Proof. From claim 3.4, for any pair of generators x_i, x_j there are unique $a, b \in X$ such that $x_i a = x_j b$, that is any pair of generators x_i, x_j has a right common multiple. Since from Proposition 3.8, M satisfies the condition (C_2), we have that x_i and x_j have a right lcm and the word $x_i a$ (or $x_j b$) represents the element $x_i \vee x_j$, since this is a common multiple of x_i and x_j of least length. So, it holds that $x_i \setminus x_j = a$ and $x_j \setminus x_i = b$, where $a, b \in X$. So, $X \cup \{\epsilon\}$ is closed under $\setminus$. □

4 Additional properties of the structure group

4.1 The right lcm of the generators is a Garside element

The braid groups and the Artin groups of finite type are Garside groups which satisfy the condition that the right lcm of their set of atoms is a Garside element. Dehornoy and Paris considered this additional condition as a part of the definition of Garside groups in [9] and in [4] it was removed from the definition. Indeed, Dehornoy gives the example of a monoid that is Garside and yet the right lcm of its atoms is not a Garside element [4]. He shows that the right lcm of the simple elements of a Garside monoid is a Garside element, where an element is *simple* if it belongs to the closure of a set of atoms under right complement and right lcm [4]. We prove the following result:

Theorem 4.1. *Let G be the structure group of a non-degenerate, involutive and braided solution (X, S) and let M be the monoid with the same presentation. Then the right lcm of the atoms (the elements of X) is a Garside element in M.*

In order to prove that, we show that the set of simple elements χ, that is the closure of X under right complement and right lcm, is equal to the closure of X under right lcm (denoted by $\overline{X}^{\vee}$), where the empty word ϵ is added. So, this implies that Δ, the right lcm of the simple elements, is the right lcm of the elements in X. We use the word reversing method developed by Dehornoy and the diagrams for word reversing. We illustrate in example 1 below the definition of the diagram and we refer the reader to [4] and [5] for more details. Here, reversing the word $u^{-1}v$ using the diagram amounts to computing a right lcm for the elements represented by u and v (see [5, p.65]).

Example 4.2. Let us consider the monoid M defined in example 2.3. We illustrate the construction of the reversing diagram.
(a) The reversing diagram of the word $x_3^{-1}x_1$ is constructed in figure 4.1 in the following way. First, we begin with the left diagram and then using the defining relation $x_1x_2 = x_3x_4$ in M, we complete it in the right diagram. We have $x_1 \setminus x_3 = x_2$ and $x_3 \setminus x_1 = x_4$.

$$\begin{tikzcd} \cdot \arrow[r, "x_1"] \arrow[d, "x_3"'] & \cdot \\ \cdot & \end{tikzcd} \qquad \begin{tikzcd} \cdot \arrow[r, "x_1"] \arrow[d, "x_3"'] & \cdot \arrow[d, "x_2"] \\ \cdot \arrow[r, "x_4"] & \cdot \end{tikzcd}$$

Figure 4.1: Reversing diagram of $x_3^{-1}x_1$

(b) The reversing diagram of the word $x_4^{-2}x_1^2$ is described in figure 4.2: we begin with the left diagram and then we complete it using the defining relations in the right diagram. So, we have $x_1^2x_2^2 = x_4^2x_3^2$ in M and since

$$\begin{tikzcd} \cdot \arrow[r, "x_1"] \arrow[d, "x_4"'] & \cdot \arrow[r, "x_1"] & \cdot \\ \cdot \arrow[d, "x_4"'] & & \\ \cdot & & \end{tikzcd} \qquad \begin{tikzcd} \cdot \arrow[r, "x_1"] \arrow[d, "x_4"'] & \cdot \arrow[r, "x_1"] \arrow[d, "x_3"] & \cdot \arrow[d, "x_2"] \\ \cdot \arrow[r, "x_2"] \arrow[d, "x_4"'] & \cdot \arrow[r, "x_4"] \arrow[d, "x_1"] & \cdot \arrow[d, "x_2"] \\ \cdot \arrow[r, "x_3"] & \cdot \arrow[r, "x_3"] & \cdot \end{tikzcd}$$

Figure 4.2: Reversing diagram of $x_4^{-2}x_1^2$

$x_1^2 = x_2^2$ and $x_3^2 = x_4^2$, it holds that $x_1^4 = x_2^4 = x_3^4 = x_4^4$ in M. So, a word representing the right lcm of x_1^2 and x_4^2 is the word x_1^4 or the word x_4^4. We obtain from the diagram that the word x_2^2 represents the element $x_1^2 \setminus x_4^2$ and the word x_3^2 represents the element $x_4^2 \setminus x_1^2$.

In order to prove that $\chi = \overline{X}^{\vee} \cup \{\epsilon\}$, we show that every complement of simple elements is the right lcm of some generators. The following technical lemma is the basis of induction for the proof of Theorem 4.1.

Lemma 4.3. (*i*) *It holds that* $M \setminus X \subseteq X \cup \{\epsilon\}$.
(*ii*) *It holds that* $M \setminus (\vee_{j=1}^{j=k} x_{i_j}) \subseteq \overline{X}^{\vee} \cup \{\epsilon\}$, *where* $x_{i_j} \in X$, $1 \leq j \leq k$.

Proof. It holds that $S(X \times X) \subseteq X \times X$, so $X \setminus X \subseteq X \cup \{\epsilon\}$ and this implies inductively *(i)* $M \setminus X \subseteq X \cup \{\epsilon\}$ (see the reversing diagram).
Let $u \in M$, then using the following rule of calculation on complements

from [4, Lemma 1.7]: for every $u, v, w \in M$, $u \setminus (v \vee w) = (u \setminus v) \vee (u \setminus w)$, we have inductively that $u \setminus (\vee_{j=1}^{j=k} x_{i_j}) = \vee_{j=1}^{j=k} (u \setminus x_{i_j})$. From (i), $u \setminus x_{i_j}$ belongs to X, so $\vee_{j=1}^{j=k} (u \setminus x_{i_j})$ is in $\overline{X}^{\vee} \cup \{\epsilon\}$. That is, (ii) holds. $\square$

Since the monoid M is Garside, the set of simples χ is finite and its construction is done in a finite number of steps in the following way:
At the $0-$th step, $\chi_0 = X$.
At the first step, $\chi_1 = X \cup \{x_i \vee x_j;\, x_i, x_j \in X\} \cup \{x_i \setminus x_j;\, x_i, x_j \in X\}$.
At the second step, $\chi_2 = \chi_1 \cup \{u \vee v;\, u, v \in \chi_1\} \cup \{u \setminus v;\, u, v \in \chi_1\}$.
We go on inductively and after a finite number of steps k, $\chi_k = \chi$.

Proposition 4.4. *It holds that* $\chi = \overline{X}^{\vee} \cup \{\epsilon\}$.

Proof. The proof is by induction on the number of steps k in the construction of χ. We show that each complement of simple elements is the right lcm of some generators. At the first step, we have that $\{x_i \setminus x_j;\text{ for all } x_i, x_j \in X\} = X \cup \{\epsilon\}$. At the following steps, we do not consider the complements of the form $... \setminus x_i$ since these belong to X (see lemma 4.3). At the second step, the complements have the following form $x_i \setminus (x_l \vee x_m)$ or $(x_i \vee x_j) \setminus (x_l \vee x_m)$ and these belong to $\overline{X}^{\vee} \cup \{\epsilon\}$ from lemma 4.3. Assume that at the $k-$th step, all the complements obtained belong to $\overline{X}^{\vee} \cup \{\epsilon\}$, that is all the elements of χ_k are right lcm of generators. At the $(k+1)-$th step, the complements have the following form $u \setminus v$, where $u, v \in \chi_k$. From the induction assumption, v is a right lcm of generators, so from lemma 4.3, $u \setminus v$ belongs to $\overline{X}^{\vee} \cup \{\epsilon\}$. $\square$

Proof of Theorem 4.1. The right lcm of the set of simples χ is a Garside element and since from Proposition 4.4, $\chi = \overline{X}^{\vee} \cup \{\epsilon\}$, we have that the right lcm of X is a Garside element. $\square$

We show now that the length of a Garside element Δ is equal to n, the cardinality of the set X. In order to show that, we prove in the following that the right lcm of k different generators has length k.

Remark 4.5. When $w \setminus x$ is not equal to the empty word, then we can interpret $w \setminus x$ in terms of the functions g_*^{-1} using the reversing diagram corresponding to the words $w = h_1 h_2 .. h_k$ and x, where $h_i, x \in X$ and for brevity of notation we write $g_i^{-1}(x)$ for $g_{h_i}^{-1}(x)$:

$$\begin{tikzcd}
\cdot \arrow[r, "h_1"] \arrow[d, "x"'] & \cdot \arrow[r, "h_2"] \arrow[d, "g_1^{-1}(x)"] & \cdot \arrow[r, dashed] \arrow[d, "g_2^{-1}g_1^{-1}(x)"] & \cdot \arrow[r, "h_k"] & \cdot \arrow[d, "g_k^{-1}\cdots g_2^{-1}g_1^{-1}(x)"] \\
\cdot \arrow[r, "g_x^{-1}(h_1)"'] & \cdot \arrow[r, "g_*^{-1}(\cdot)"'] & \cdot \arrow[r, dashed] & \cdot \arrow[r, "g_{**}^{-1}(\cdot)"'] & \cdot
\end{tikzcd}$$

That is, $h_1h_2..h_k \setminus x = g_k^{-1}..g_2^{-1}g_1^{-1}(x)$ and this is equal to $g_w^{-1}(x)$, since the action on X is a right action. Having a glance at the reversing diagram, we remark that if $w \setminus x$ is not equal to the empty word, then none of the complements $h_1 \setminus x$, $h_1h_2 \setminus x$,.., $h_1h_2..h_{k-1} \setminus x$ can be equal to the empty word.

Lemma 4.6. *Let h_i, x be all different elements in X, for $1 \leq i \leq k$. Then $(\vee_{i=1}^{i=k} h_i) \setminus x$ is not equal to the empty word ϵ.*

Proof. By induction on k. If $k = 1$, then $h_1 \setminus x \neq \epsilon$, as $h_1 \neq x$.
Now assume $(\vee_{i=1}^{i=k-1} h_i) \setminus x \neq \epsilon$ and assume by contradiction that $(\vee_{i=1}^{i=k} h_i) \setminus x = \epsilon$. Using the following rule of computation on the complement from [4, Lemma 1.7]: $(u \vee v) \setminus w = (u \setminus v) \setminus (u \setminus w)$, we have $(\vee_{i=1}^{i=k} h_i) \setminus x = (\vee_{i=1}^{i=k-1} h_i \vee h_k) \setminus x = ((\vee_{i=1}^{i=k-1} h_i) \setminus h_k) \setminus ((\vee_{i=1}^{i=k-1} h_i) \setminus x)$. From the induction assumption, $(\vee_{i=1}^{i=k-1} h_i) \setminus x \neq \epsilon$ and $(\vee_{i=1}^{i=k-1} h_i) \setminus h_k \neq \epsilon$, so $(\vee_{i=1}^{i=k} h_i) \setminus x = \epsilon$ implies that $(\vee_{i=1}^{i=k-1} h_i) \setminus h_k = (\vee_{i=1}^{i=k-1} h_i) \setminus x$. Assume w represents the element $\vee_{i=1}^{i=k-1} h_i$, then from remark 4.5, $w \setminus h_k$ can be interpreted as $g_w^{-1}(h_k)$ and $w \setminus x$ can be interpreted as $g_w^{-1}(x)$. The function g_w^{-1} is a bijective function as it is the composition of bijective functions, so $g_w^{-1}(h_k) = g_w^{-1}(x)$ implies that $h_k = x$, but this is a contradiction. So, $(\vee_{i=1}^{i=k} h_i) \setminus x \neq \epsilon$. $\square$

Theorem 4.7. *Let G be the structure group of a non-degenerate, braided and involutive solution (X, S), where $X = \{x_1, .., x_n\}$ and let M be the monoid with the same presentation. Let Δ be a Garside element in M. Then the length of Δ is n.*

Proof. From theorem 4.1, Δ represents the right lcm of the elements in X, that is $\Delta = x_1 \vee x_2 \vee ... \vee x_n$ in M. We show by induction that a word representing the right lcm $x_{i_1} \vee x_{i_2} \vee .. \vee x_{i_k}$ has length k, where $x_{i_j} \neq x_{i_l}$ for $j \neq l$. If $k = 2$, then there are different generators a, b such that $S(x_{i_1}, a) = (x_{i_2}, b)$, so $x_{i_1}a = x_{i_2}b$ is a relation in M and the right lcm of x_{i_1}, x_{i_2} has length 2. Assume that the right lcm $x_{i_1} \vee x_{i_2} \vee .. \vee x_{i_{k-1}}$ has length $k-1$. Then the right lcm $x_{i_1} \vee x_{i_2} \vee .. \vee x_{i_{k-1}} \vee x_{i_k}$ is obtained from the reversing diagram corresponding to the words $x_{i_1} \vee x_{i_2} \vee .. \vee x_{i_{k-1}}$ and x_{i_k}. From lemma 4.6, $(x_{i_1} \vee x_{i_2} \vee .. \vee x_{i_{k-1}}) \setminus x_{i_k}$ is not equal to the empty word, so from lemma 4.3 it has length 1. So, the right lcm $x_{i_1} \vee x_{i_2} \vee .. \vee x_{i_k}$ has length k and this implies that $x_1 \vee x_2 \vee .. \vee x_n$ has length n. $\square$

4.2 Homological dimension

Dehornoy and Laffont construct a resolution of $\mathbb{Z}$ (as trivial $\mathbb{Z}M$-module) by free $\mathbb{Z}M$-modules, when M satisfies some conditions [8]. Moreover, they

show that every Garside group is of type FL, that is with a finite resolution [8, Prop. 2.9-2.10]. Charney, Meier, and Whittlesey show in [1] that Garside groups have finite homological dimension, using another approach. In [8], Dehornoy and Laffont show that whenever M is a Garside monoid then the resolution defined in [1] is isomorphic to the resolution they define. We use the following result from [8] in order to show that the homological dimension of the structure group corresponding to a set-theoretical solution (X, S) of the quantum Yang-Baxter equation is equal to the number of generators in X.

Proposition 4.8. *[8, Cor.3.6] Assume that M is a locally Gaussian monoid admitting a generating set χ such that $\chi \cup \{\epsilon\}$ is closed under left and right complement and lcm and such that the norm of every element in χ is bounded above by n. Then the (co)homological dimension of M is at most n.*

Using Proposition 4.8, we prove the following result:

Theorem 4.9. *Let (X, S) be a set-theoretical solution of the quantum Yang-Baxter equation, where $X = \{x_1, .., x_n\}$ and (X, S) is non-degenerate, braided and involutive. Let G be the structure group corresponding to (X, S). Then the (co)homological dimension of G is equal to n, the number of generators in X.*

Proof. The set of simples χ satisfies the conditions of Corollary 4.8 and the norm of every element in χ is bounded by n, since this is the length of the right lcm of χ (from Theorems 4.1 and 4.7). So, the (co)homological dimension of G is is equal to n. □

Remark 4.10. It was pointed to us by P.Etingof that this result can be also proved differently: by showing that the classifying space of the structure group G is a compact manifold of dimension n (as there is a free action of G on R^X).

5 Structure groups and indecomposable solutions

Picantin defines the notion of Δ-pure Garside monoid M in [16] and he shows there that the center of M is the infinite cyclic submonoid generated by some power of Δ. We find in this section conditions under which a monoid is Δ-pure Garside in terms of set-theoretical solutions.

5.1 Δ-pure Garside monoids

Let χ be the set of simples and Δ a Garside element in M. The *exponent* of M is the order of the automorphism ϕ, where ϕ is the extension of the function $x \to (x \setminus \Delta) \setminus \Delta$ from χ into itself.

Definition 5.1. [16] The monoid M is $\Delta-$*pure* if for every x, y in X, it holds that $\Delta_x = \Delta_y$, where $\Delta_x = \vee\{b \setminus x; b \in M\}$ and $\vee$ denotes the right lcm.

Picantin shows that if M is a Δ-pure Garside monoid with exponent e and group of fractions G, then the center of M (resp. of G) is the infinite cyclic submonoid (resp. subgroup) generated by Δ^e. Let consider the following example, to illustrate these definitions.

Example 5.2. Let $X = \{x_1, x_2, x_3\}$ and let $S(x_i, x_j) = (f(j), f^{-1}(i))$, where $f = (1, 2, 3)$, be a non-degenerate, braided and involutive set-theoretical solution. Let M be the monoid with the same presentation as the structure group of (X, S), the defining relations in M are then: $x_1^2 = x_2x_3$, $x_2^2 = x_3x_1$ and $x_3^2 = x_1x_2$. So, $X \setminus x_1 = \{x_3\}$, $X \setminus x_2 = \{x_1\}$ and $X \setminus x_3 = \{x_2\}$. Using the reversing diagram, we obtain inductively that $M \setminus x_i = X \cup \{\epsilon\}$ for $1 \leq i \leq 3$, that is M is Δ-pure Garside, since $\Delta_1 = \Delta_2 = \Delta_3$. As an example, $x_2 \setminus x_1 = x_3$, so $x_2x_1 \setminus x_1 = x_2$ and so $x_2x_1x_3 \setminus x_1 = x_1$ that is $X \cup \{\epsilon\} \subseteq M \setminus x_1$ and since $M \setminus x_1 \subseteq X \cup \{\epsilon\}$ (see lemma 4.3) we have the equality. Each word x_i^3 for $i = 1, 2, 3$ represents a Garside element, denoted by Δ. The set of simples is $\chi = \{\epsilon, x_1, x_2, x_3, x_1^2, x_2^2, x_3^2, \Delta\}$. The exponent of M is equal to 1, since the function $x \to (x \setminus \Delta) \setminus \Delta$ from χ to itself is the identity. As an example, the image of x_1 is $(x_1 \setminus \Delta) \setminus \Delta = x_1^2 \setminus \Delta = x_1$, the image of x_2^2 is $(x_2^2 \setminus \Delta) \setminus \Delta = x_2 \setminus \Delta = x_2^2$ and so on. So, the center of the structure group of (X, S) is cyclic and generated by Δ, using the result of Picantin.

5.2 Structure groups and indecomposable solutions

A non-degenerate, braided and involutive set-theoretical solution (X, S) is said to be *decomposable* if X is a union of two nonempty disjoint non-degenerate invariant subsets, where an *invariant* subset Y is a set that satisfies $S(Y \times Y) \subseteq Y \times Y$. Otherwise, (X, S) is said to be *indecomposable*. Etingof et al give a classification of non-degenerate, braided and involutive solutions with X up to 8 elements, considering their decomposability and other properties [11]. Rump proves Gateva-Ivanova's conjecture that every

square-free, non-degenerate, involutive and braided solution (X,S) is decomposable, whenever X is finite. Moreover, he shows that an extension to infinite X is false [19]. We find a criterion for decomposability of the solution involving the Garside structure of the structure group (monoid), that is we prove the following result.

Theorem 5.3. *Let G be the structure group of a non-degenerate, braided and involutive solution (X,S) and let M be the monoid with the same presentation. Then M is Δ-pure Garside if and only if (X,S) is indecomposable.*

In what follows, we use the notation from [16]: for $X, Y \subseteq M$, $Y \setminus X$ denotes the set of elements $b \setminus a$ for $a \in X$ and $b \in Y$. We write $Y \setminus a$ for $Y \setminus \{a\}$ and $b \setminus X$ for $\{b\} \setminus X$. We need the following lemma for the proof of Theorem 5.3

Lemma 5.4. *Let (X,S) be the union of non-degenerate invariant subsets Y and Z. Then $M \setminus Y \subseteq Y \cup \{\epsilon\}$ and $M \setminus Z \subseteq Z \cup \{\epsilon\}$.*

Proof. If Y is an invariant subset of X, then $Y \setminus Y \subseteq Y \cup \{\epsilon\}$, since $S(Y \times Y) \subseteq Y \times Y$. From [11, Proposition 2.15], the map S defines bijections $Y \times Z \to Z \times Y$ and $Z \times Y \to Y \times Z$. So, $S(Y \times Z) \subseteq Z \times Y$ and $S(Z \times Y) \subseteq Y \times Z$, and this implies $Z \setminus Y \subseteq Y$. That is, we have that $Y \setminus Y \subseteq Y \cup \{\epsilon\}$ and $Z \setminus Y \subseteq Y$, so $X \setminus Y \subseteq Y \cup \{\epsilon\}$ and this implies inductively that $M \setminus Y \subseteq Y \cup \{\epsilon\}$ (see the reversing diagram). The same holds for Z. $\square$

Proof of Theorem 5.3. Assume (X,S) is decomposable, that is (X,S) is the union of non-degenerate invariant subsets Y and Z. From lemma 5.4, we have $M \setminus Y \subseteq Y \cup \{\epsilon\}$ and $M \setminus Z \subseteq Z \cup \{\epsilon\}$. Let $y \in Y$ and $z \in Z$, then $\Delta_y = \vee(M \setminus y)$ cannot be the same as $\Delta_z = \vee(M \setminus z)$. So, M is not Δ-pure Garside .
Assume M is not Δ-pure Garside. Let $x_k \in X$, we denote by Y_k the set $(M \setminus x_k)$ from which we remove $\{\epsilon\}$. So, $\Delta_{x_k} = \vee(Y_k)$, where Y_k is a subset of X from Lemma 4.3. Let x_i, x_j be in X, then from [16], either $\Delta_{x_i} = \Delta_{x_j}$ or the left gcd of Δ_{x_i} and Δ_{x_j} is ϵ. If $\Delta_{x_i} = \Delta_{x_j}$, then $Y_i = Y_j$ and if the left gcd of Δ_{x_i} and Δ_{x_j} is ϵ, then Y_i and Y_j are disjoint subsets of X. Since M is not Δ-pure Garside, there exist x_{i_1}, x_{i_2}, .., x_{i_m} in X such that Y_{i_1}, Y_{i_2},.., Y_{i_m} are disjoint subsets of X. Moreover, $X = Y_{i_1} \cup Y_{i_2} \cup .. \cup Y_{i_m}$, since each $x \in X$ is equal to an element $x_k \setminus x_i$ for some $x_k, x_i \in X$ (from the existence of left lcms). We show that Y_{i_j} is an invariant subset of X, that is $S(Y_{i_j}, Y_{i_j}) \subseteq (Y_{i_j}, Y_{i_j})$. Let $x \in X$ and $y \in Y_{i_j}$, then $x \setminus y = x \setminus (w \setminus x_{i_j})$, for some $w \in M$. Using the following rule of computation on the complement

from [4, Lemma 1.7]: $x \setminus (u \setminus v) = (ux) \setminus v$, we have $x \setminus y = (wx) \setminus x_{i_j}$, that is $x \setminus y$ belongs to Y_{i_j}. In particular, if $x \in Y_{i_j}$ then $S(x, y') = (y, y'')$, where $y', y'' \in Y_{i_j}$. So, Y_{i_j} is an invariant subset of X for $1 \leq j \leq m$ and this implies that (X, S) is decomposable. $\square$

6 From Garside groups to structure groups

We establish the converse implication in the one-to-one correspondence between the Garside groups and the structure groups, that is we prove the following:

Theorem 6.1. *Let* $\mathrm{Mon}\langle X \mid R\rangle$ *be a Garside monoid such that:*
(i) There are $n(n-1)/2$ *relations in* R*, where* n *is the cardinality of* X*, and each side of a relation in* R *has length 2.*
(ii) If the word $x_i x_j$ *appears in* R*, then it appears only once.*
Then there exists a function $S : X \times X \to X \times X$ *such that* (X, S) *is a non-degenerate, involutive and braided set-theoretical solution and* $\mathrm{Gp}\langle X \mid R\rangle$ *is its structure group.*
If additionally: (iii) There is no word x_i^2 *in* R*, then* (X, S) *is square-free.*

6.1 Proof of Theorem 6.1

In order to prove Theorem 6.1, we use the concepts of left lcm and left coherence from [4] and [8], but we do not use exactly the same notations. The notation for the *left lcm of* x *and* y is $z = x \widetilde{\vee} y$ and for *the complement at left of* y *on* x the notation is $x \widetilde{\backslash} y$, where $x \widetilde{\vee} y = (x \widetilde{\backslash} y) y$.

Definition 6.2. [8] Let M be a monoid. The *left coherence condition* on M is satisfied if it holds for any $x, y, z \in M$: $((x \widetilde{\backslash} y) \widetilde{\backslash} (z \widetilde{\backslash} y)) \widetilde{\backslash} ((x \widetilde{\backslash} z) \widetilde{\backslash} (y \widetilde{\backslash} z)) \equiv^+ \epsilon$.

This property is also called the *left cube condition.* We show that if (X, S) is a non-degenerate and involutive set-theoretical solution, then (X, S) is braided if and only if X is coherent and left coherent. The left coherence of X is satisfied if the following condition on all x_i, x_j, x_k in X is satisfied: $(x_i \widetilde{\backslash} x_j) \widetilde{\backslash} (x_k \widetilde{\backslash} x_j) = (x_i \widetilde{\backslash} x_k) \widetilde{\backslash} (x_j \widetilde{\backslash} x_k)$, where the equality is in the free monoid since the complement on the left is totally defined and its range is X. Note that as in the proof of the coherence, left coherence on X implies left coherence on M, since the monoid M is atomic. Clearly, the following implication is derived from Theorem 3.3:

Lemma 6.3. *Assume* (X, S) *is non-degenerate and involutive. If* (X, S) *is braided, then* X *is coherent and left coherent.*

The proof of the converse implication is less trivial and requires a lot of computations. Before we proceed, we first express the left complement in terms of the functions f_i that define (X,S). As the proofs are symmetric to those done in Section 3.2 with the right complement we omit them.

Lemma 6.4. *Assume (X,S) is non-degenerate. Let x_i, x_j be different elements in X. Then $x_j \widetilde{\backslash} x_i = f_i^{-1}(j)$.*

Lemma 6.5. *Assume (X,S) is non-degenerate and involutive. Let x_i, x_k be elements in X. Then $f_k^{-1}(i) = g_{f_i^{-1}(k)}(i)$.*

Lemma 6.6. *Assume (X,S) is non-degenerate. If X is coherent and left coherent, then for every i,j,k the following equations hold:*
(A) $f_j f_{f_j^{-1}(k)} = f_k f_{f_k^{-1}(j)}$
(B) $g_i g_{g_i^{-1}(k)} = g_k g_{g_k^{-1}(i)}$

Proof. From lemma 6.4, we have for all different $1 \leq i,j,k \leq n$ that $(x_i \widetilde{\backslash} x_j) \widetilde{\backslash} (x_k \widetilde{\backslash} x_j) = f^{-1}_{f_j^{-1}(k)} f_j^{-1}(i)$ and $(x_i \widetilde{\backslash} x_k) \widetilde{\backslash} (x_j \widetilde{\backslash} x_k) = f^{-1}_{f_k^{-1}(j)} f_k^{-1}(i)$. If X is left coherent, then for all different $1 \leq i,j,k \leq n$, we have $(*)$ $f^{-1}_{f_j^{-1}(k)} f_j^{-1}(i) = f^{-1}_{f_k^{-1}(j)} f_k^{-1}(i)$. If $j = k$, the equality (A) holds trivially, so let fix j and k such that $j \neq k$. We denote $F_1 = f^{-1}_{f_j^{-1}(k)} f_j^{-1}$ and $F_2 = f^{-1}_{f_k^{-1}(j)} f_k^{-1}$, these functions are bijective, since these are compositions of bijective functions and satisfy $F_1(i) = F_2(i)$ whenever $i \neq j,k$. It remains to show that $F_1(k) = F_2(k)$ and $F_1(j) = F_2(j)$. Assume by contradiction that $F_1(k) = F_2(j)$ and $F_1(j) = F_2(k)$, so there is $1 \leq m \leq n$ such that $m = f^{-1}_{f_j^{-1}(k)} f_j^{-1}(k) = f^{-1}_{f_k^{-1}(j)} f_k^{-1}(j)$, that is $f_{f_j^{-1}(k)}(m) = f_j^{-1}(k)$ and $f_{f_k^{-1}(j)}(m) = f_k^{-1}(j)$. That is $S(m, f_j^{-1}(k)) = (m, f_j^{-1}(k))$ and $S(m, f_k^{-1}(j)) = (m, f_k^{-1}(j))$, since (X,S) is involutive. So, $g_m(f_j^{-1}(k)) = m$ and $g_m(f_k^{-1}(j)) = m$. Since g_m is bijective, this implies that there is $1 \leq l \leq n$ such that $l = f_j^{-1}(k) = f_k^{-1}(j)$, that is $S(l,j) = (l,k)$. But, since $j \neq k$, this contradicts the fact that (X,S) is involutive. So, since the functions $f_.$ are bijective, (*) is equivalent to (A). Equation (B) is obtained in the same way using the coherence of X (see lemma 3.6). $\square$

Proposition 6.7. *Let (X,S) be a non-degenerate and involutive set-theoretical solution. If X is coherent and left coherent, then (X,S) is braided.*

Proof. We need to show that the functions f_i and g_i satisfy the following equations from lemma 3.1:

(i) $f_j f_i = f_{f_j(i)} f_{g_i(j)}$, $1 \le i, j \le n$.
(ii) $g_i g_j = g_{g_i(j)} g_{f_j(i)}$, $1 \le i, j \le n$.
(iii) $f_{g_{f_l(m)}(j)} g_m(l) = g_{f_{g_l(j)}(m)} f_j(l)$, $1 \le j, l, m \le n$.
From lemma 6.6, we have for $1 \le j, k \le n$ that (A) $f_j f_{f_j^{-1}(k)} = f_k f_{f_k^{-1}(j)}$. Assume $m = f_j^{-1}(k)$, that is $k = f_j(m)$ and we replace in formula (A) $f_j^{-1}(k)$ by m and k by $f_j(m)$, then we obtain $f_j f_m = f_{f_j(m)} f_{f^{-1}_{f_j(m)}(j)}$. In order to show that (i) holds, we show that $f^{-1}_{f_j(m)}(j) = g_m(j)$. From lemma 6.5, we have $f_l^{-1}(j) = g_{f_j^{-1}(l)}(j)$ for every j, l, so by replacing l by $f_j(m)$, we obtain $f^{-1}_{f_j(m)}(j) = g_m(j)$. So, (i) holds.
From Corollary 6.6, we have for $1 \le j \ne k \le n$ that (B) $g_i g_{g_i^{-1}(k)} = g_k g_{g_k^{-1}(i)}$. Assume $m = g_i^{-1}(k)$, that is $k = g_i(m)$ and we replace in formula (B) $g_i^{-1}(k)$ by m and k by $g_i(m)$, then we obtain $g_i g_m = g_{g_i(m)} g_{g^{-1}_{g_i(m)}(i)}$. In order to show that (ii) holds, we show that $g^{-1}_{g_i(m)}(i) = f_m(i)$. From lemma 3.7, we have $g_l^{-1}(i) = f_{g_i^{-1}(l)}(i)$, so by replacing l by $g_i(m)$, we obtain $g^{-1}_{g_i(m)}(i) = f_m(i)$. So, (ii) holds.
It remains to show that (iii) holds. From (i), we have for $1 \le i, j \le n$ that $f_j f_i = f_{f_j(i)} f_{g_i(j)}$ and this is equivalent to $f_{g_i(j)} = f^{-1}_{f_j(i)} f_j f_i$. We replace i by $f_l(m)$ for some $1 \le l, m \le n$ in the formula. We obtain $f_{g_{f_l(m)}(j)} = f^{-1}_{f_j f_l(m)} f_j f_{f_l(m)}$. By applying these functions on $g_m(l)$ on both sides, we obtain $f_{g_{f_l(m)}(j)} g_m(l) = f^{-1}_{f_j f_l(m)} f_j f_{f_l(m)} g_m(l)$. Since (X, S) is involutive, we have $f_{f_l(m)} g_m(l) = l$ (see lemma 3.1). So, $f_{g_{f_l(m)}(j)} g_m(l) = f^{-1}_{f_j f_l(m)} f_j(l)$. From lemma 6.5, we have $f_i^{-1}(k) = g_{f_k^{-1}(i)}(k)$ for every i, k, so replacing i by $f_j f_l(m)$ and k by $f_j(l)$ gives $f^{-1}_{f_j f_l(m)}(f_j(l)) = g_{f^{-1}_{f_j(l)} f_j f_l(m)}(f_j(l))$. So, $f_{g_{f_l(m)}(j)} g_m(l) = g_{f^{-1}_{f_j(l)} f_j f_l(m)}(f_j(l))$. From (i), we have that $f^{-1}_{f_j(l)} f_j f_l(m) = f_{g_l(j)}(m)$, so $f_{g_{f_l(m)}(j)} g_m(l) = g_{f_{g_l(j)}(m)} f_j(l)$, that is (iii) holds. $\square$

Proof of Theorem 6.1. First, we define a function $S : X \times X \to X \times X$ and $2n$ functions f_i, g_i for $1 \le i \le n$, such that $S(i, j) = (g_i(j), f_j(i))$ in the following way: if there is a relation $x_i x_j = x_k x_l$ then we define $S(i, j) = (k, l)$, $S(k, l) = (i, j)$ and we define $g_i(j) = k$, $f_j(i) = l$, $g_k(l) = i$ and $f_l(k) = j$. If the word $x_i x_j$ does not appear as a side of a relation, then we define $S(i, j) = (i, j)$ and we define $g_i(j) = i$ and $f_j(i) = j$. We show that the functions f_i and g_i are well defined for $1 \le i \le n$: assume $g_i(j) = k$ and $g_i(j) = k'$ for some $1 \le j, k, k' \le n$ and $k \ne k'$, then it means from the definition of S that $S(i, j) = (k, .)$ and $S(i, j) = (k', ..)$ that is the word $x_i x_j$

appears twice in R and this contradicts (ii). The same argument holds for the proof that the functions f_i are well defined.
We show that the functions f_i and g_i are bijective for $1 \leq i \leq n$: assume $g_i(j) = k$ and $g_i(j') = k$ for some $1 \leq j, j', k \leq n$ and $j \neq j'$, then from the definition of S we have $S(i, j) = (k, l)$ and $S(i, j') = (k, l')$ for some $1 \leq l, l' \leq n$, that is there are the following two defining relations in R: $x_i x_j = x_k x_l$ and $x_i x_{j'} = x_k x_{l'}$. But this means that x_i and x_k have two different right lcms and this contradicts the assumption that the monoid is Garside. So, these functions are injective and since X is finite they are bijective. Assuming f_i not injective yields generators with two different left lcms. So, S is well-defined and (X, S) is non-degenerate and from (ii) (X, S) is also involutive. It remains to show that (X, S) is braided: since $\mathrm{Mon}\langle X \mid R\rangle$ is Garside, it is coherent and left coherent so from lemma 6.7, (X, S) is braided. Obviously condition (iii) implies that (X, S) is also square-free. □

6.2 The one-to-one correspondence

It remains to establish the one-to-one correspondence between structure groups of non-degenerate, involutive and braided set-theoretical solutions of the quantum Yang-Baxter equation and a class of Garside groups admitting a certain presentation and in order to that we need the following terminology and claims.

Definition 6.8. A *tableau monoid* is a monoid $\mathrm{Mon}\langle X \mid R\rangle$ satisfying the condition that each side of a relation in R has length 2.

Definition 6.9. We say that two tableau monoids $\mathrm{Mon}\langle X \mid R\rangle$ and $\mathrm{Mon}\langle X' \mid R'\rangle$ are *t-isomorphic* if there exists a bijection $s : X \to X'$ such that $x_i x_j = x_k x_l$ is a relation in R if and only if $s(x_i)s(x_j) = s(x_k)s(x_l)$ is a relation in R'.

Clearly, if two tableau monoids are t-isomorphic then they are isomorphic and the definition is enlarged to groups. Set-theoretical solutions (X, S) and (X', S') are *isomorphic* if there exists a bijection $\phi : X \to X'$ which maps S to S', that is $S'(\phi(x), \phi(y)) = (\phi(S_1(x, y)), \phi(S_2(x, y)))$.

Proposition 6.10. *Let (X, S) and (X', S') be non-degenerate, involutive and braided set-theoretical solutions. Assume (X, S) and (X', S') are isomorphic. Then their structure groups (monoids) G and G' are t-isomorphic tableau groups (monoids). Conversely, if* $\mathrm{Mon}\langle X \mid R\rangle$ *and* $\mathrm{Mon}\langle X \mid R'\rangle$ *are t-isomorphic tableau Garside monoids each satisfying the conditions* (i)

and (ii) from Theorem 6.1, then the solutions (X, S) and (X', S') defined respectively by $\mathrm{Mon}\langle X \mid R\rangle$ *and* $\mathrm{Mon}\langle X \mid R'\rangle$ *are isomorphic.*

Proof. Clearly, the structure groups (monoids) G and G' are tableau groups (monoids). We need to show that G and G' are t-isomorphic. Since (X, S) and (X', S') are isomorphic, there exists a bijection $\phi : X \to X'$ which maps S to S', that is $S'(\phi(x), \phi(y)) = (\phi(S_1(x, y)), \phi(S_2(x, y)))$. So, since by definition $S(x, y) = (S_1(x, y), S_2(x, y))$, we have $xy = tz$ if and only if $\phi(x)\phi(y) = \phi(t)\phi(z)$. That is, if we take s to be equal to ϕ we have that G and G' are t-isomorphic. For the converse, take ϕ to be equal to s and from the definition of S and S' from their tableau we have $S'(\phi(x), \phi(y)) = (\phi(S_1(x, y)), \phi(S_2(x, y)))$, that is (X, S) and (X', S') are isomorphic. $\square$

7 The structure group of a permutation solution

In this part, we consider a special case of set-theoretical solutions of the quantum Yang-Baxter equation, namely the permutation solutions. These solutions were defined by Lyubashenko (see [11]). Let X be a set and let $S : X^2 \to X^2$ be a mapping. A permutation solution is a set-theoretical solution of the form $S(x, y) = (g(y), f(x))$, where $f, g : X \to X$. The solution (X, S) is nondegenerate iff f, g are bijective, (X, S) is braided iff $fg = gf$ and (X, S) is involutive iff $g = f^{-1}$. Note that these solutions are defined by only two functions, while for a general set-theoretical solution the number of defining functions is twice the cardinality of the set X.

7.1 About permutation solutions that are non-involutive

In this subsection, we consider the special case of non-degenerate and braided permutation solutions that are not necessarily involutive and we show that their structure group is Garside.

Let X be a finite set and let $S : X^2 \to X^2$ be defined by $S(x, y) = (g(y), f(x))$, where $f, g : X \to X$ are bijective and satisfy $fg = gf$. So, (X, S) is a non-degenerate and braided permutation solution that is not necessarily involutive, as we do not require $g = f^{-1}$. Let G be the structure group of (X, S) and let M be the monoid with the same presentation. We define an equivalence relation on the set X in the following way:
$x \equiv x'$ if and only if there is an integer k such that $(fg)^k(x) = x'$. We define $X' = X/\equiv$ and we define functions $f', g' : X' \to X'$ such that $f'([x]) = [f(x)]$ and $g'([x]) = [g(x)]$, where $[x]$ denotes the equivalence class of x modulo $\equiv$. We then define $S' : X' \times X' \to X' \times X'$ by $S'([x], [y]) =$

$(g'([y]), f'([x])) = ([g(y)], [f(x)])$. Our aim is to show that (X', S') is a well-defined non-degenerate, involutive and braided solution (a permutation solution) and that its structure group G' is isomorphic to G. Before doing this, we illustrate the main ideas of the proofs to come with an example.

Example 7.1. $X = \{x_1, x_2, x_3, x_4, x_5\}$ and let $f = (1,4)(2,3)$ and $g = (1,2)(3,4)$. Then f, g are bijective and satisfy $fg = gf = (1,3)(2,4)$ but $fg \neq Id$, so (X, S) is a non-degenerate and braided (permutation) solution, where $S(x, y) = (g(y), f(x))$. The set of relations R is:

$$\begin{array}{ll} x_1^2 = x_2x_4 = x_3^2 = x_4x_2 & x_1x_2 = x_1x_4 = x_3x_4 = x_3x_2 \\ x_2^2 = x_1x_3 = x_4^2 = x_3x_1 & x_1x_5 = x_5x_4 = x_3x_5 = x_5x_2 \\ x_2x_1 = x_2x_3 = x_4x_3 = x_4x_1 & x_2x_5 = x_5x_3 = x_4x_5 = x_5x_1 \end{array}$$

Using $\equiv$ defined above, we have $X' = \{[x_1], [x_2], [x_5]\}$, with $x_1 \equiv x_3$ and $x_2 \equiv x_4$, since in this example it holds that $fg(1) = 3$ and $fg(2) = 4$. Applying the definition of S' yields $S'([x_1], [x_1]) = ([g(1)], [f(1)]) = ([2], [4]) = ([2], [2])$ and so on. So, $G' = \mathrm{Gp}\langle [x_1], [x_2], [x_5] \mid [x_1]^2 = [x_2]^2, [x_1][x_5] = [x_5][x_2], [x_2][x_5] = [x_5][x_1] \rangle$. Note that in G, it holds that $x_1 = x_3$ and $x_2 = x_4$ since many of the defining relations from R involve cancellation and $G = \mathrm{Gp}\langle x_1, x_2, x_5 \mid x_1^2 = x_2^2, x_1x_5 = x_5x_2, x_2x_5 = x_5x_1 \rangle$. So, G and G' have the same presentation, up to a renaming of the generators.

Before we proceed to the general case, we need the following general lemma. The proof, by induction on k, is omitted because it is straightforward and technical (see [2]).

Lemma 7.2. *If k is even, then $S^k(x, y) = (f^{k/2}g^{k/2}(x), f^{k/2}g^{k/2}(y))$.*
If k is odd, then $S^k(x, y) = (f^{(k-1)/2}g^{(k+1)/2}(y), f^{(k+1)/2}g^{(k-1)/2}(x))$.

Lemma 7.3. *Let $x, x' \in X$. If $x \equiv x'$, then x and x' are equal in G.*

Proof. Let x, x' be in X such that $x \equiv x'$. If $x \equiv x'$ then it means that there is an integer k such that $(fg)^k(x) = f^kg^k(x) = x'$. If k is odd, then let y in X be defined in the following way: $y = f^{(k+1)/2}g^{(k-1)/2}(x)$. So, from lemma 7.2, $S^k(x, y) = (f^{(k-1)/2}g^{(k+1)/2}(y), f^{(k+1)/2}g^{(k-1)/2}(x)) = (f^{(k-1)/2}g^{(k+1)/2}f^{(k+1)/2}g^{(k-1)/2}(x), y) = ((fg)^k(x), y) = (x', y)$. So, there is a relation $xy = x'y$ in G which implies that $x = x'$ in G. If k is even and $(fg)^k(x) = x'$, then there is an element $x'' \in X$ such that $(fg)^{k-1}(x) = x''$, where $k-1$ is odd. So, from the subcase studied above, there is $y \in X$, $y = f^{k/2}g^{(k-2)/2}(x)$, such that there is a relation $xy = x''y$ in G and this implies that $x = x''$ in G. Additionally, $(fg)(x'') = x'$, so from the same argument as above there is $z \in X$ such that there is a relation $x'z = x''z$ in G and this implies that $x' = x''$ in G. So, $x = x'$ in G. ∎

We now show that (X', S') is a well-defined non-degenerate, involutive and braided solution and this implies from Theorem 3.3 that its structure group G' is Garside.

Lemma 7.4. *(i) f' and g' are well defined, so S' is well-defined.*
(ii) f' and g' are bijective, so S' is non-degenerate.
(iii) f' and g' satisfy $f'g' = g'f'$, so S' is braided.
(iv) f' and g' satisfy $f'g' = g'f' = id_{X'}$, so S' is involutive.

Proof. (i) Let x, x' be in X such that $x \equiv x'$. We show that $f'([x']) = f'([x])$, that is $[f(x')] = [f(x)]$. Since $x \equiv x'$, there is an integer k such that $x' = (fg)^k(x)$, so $f'([x']) = [f(x')] = [f(fg)^k(x)] = [(fg)^k f(x)] = [f(x)] = f'([x])$, using the fact that $fg = gf$. The same proof holds for $g'([x']) = g'([x])$.
(ii) Assume that there are $x, y \in X$ such that $f'([x]) = f'([y])$, that is $[f(x)] = [f(y)]$. By the definition of $\equiv$, this means that there is an integer k such that $f(x) = (fg)^k f(y)$, that is $f(x) = f(fg)^k(y)$, since $fg = gf$. But f is bijective, so $x = (fg)^k(y)$, which means that $[x] = [y]$. The same proof holds for g', using the fact that g is bijective.
(iii) Let $[x] \in X'$, so $f'(g'([x])) = f'([g(x)]) = [f(g(x))]$ and $g'f'([x]) = g'([f(x)]) = [g(f(x))]$. Since $fg = gf$, $f'g' = g'f'$.
(iv) Let $[x] \in X'$, so from the definition of $\equiv$, we have $[fg(x)] = [x]$, so $f'g'([x]) = [x]$, that is $f'g' = id_{X'}$. □

Lemma 7.5. *Let (X, S) be a not necessarily involutive permutation solution. Let $X' = X/\equiv$ and let G' be the structure group corresponding to (X', S'), as defined above. Then G' is Garside. Furthermore, if $x_i x_j = x_k x_l$ is a defining relation in G, then $[x_i][x_j] = [x_k][x_l]$ is a defining relation in G'.*

Proof. It holds that (X', S') is a non-degenerate, braided and involutive permutation solution, so by Theorem 3.3 the group G' is Garside. Assume that $x_i x_j = x_k x_l$ is a defining relation in G, that is $S(x_i, x_j) = (x_k, x_l)$. From the definition of S', $S'([x_i], [x_j]) = ([g(x_j)], [f(x_i)]) = ([x_k], [x_l])$, that is there is a defining relation $[x_i][x_j] = [x_k][x_l]$ in G'. Note that this relation may be a trivial one if $[x_i] = [x_k]$ and $[x_j] = [x_l]$ in G' □

Now, it remains to show that the structure group G is isomorphic to the group G'.

Theorem 7.6. *Let G be the structure group of a non-degenerate and braided permutation solution (X, S) that is not necessarily involutive. Then G is a Garside group.*

Proof. We show that the group G is isomorphic to the group G', where G' is the structure group of (X', S') and $X' = X/\equiv$, and from lemma 7.5 this implies that G is a Garside group. Let $\Phi : X \to X'$ be the quotient map defined by $\Phi(x) = [x]$ for all $x \in X$. From lemma 7.5, $\Phi : G \to G'$ is an homomorphism of groups, so Φ is an epimorphism. We need to show that Φ is injective. We show that if $[x][y] = [t][z]$ is a non-trivial defining relation in G', then $xy = tz$ is a defining relation in G. If $[x][y] = [t][z]$ is a non-trivial defining relation in G', then since $S'([x], [y]) = ([g(y)], [f(x)])$, we have that $[g(y)] = [t]$ and $[f(x)] = [z]$. That is, there are $z' \in [z]$ and $t' \in [t]$ such that $g(y) = t'$ and $f(x) = z'$. This implies that $S(x, y) = (g(y), f(x)) = (t', z')$, that is $xy = t'z'$ is a defining relation in G. It holds that $t \equiv t'$ and $z \equiv z'$, so from lemma 7.3, $t = t'$ and $z = z'$ in G. So, $xy = tz$ is a defining relation in G.
Note that if $[x][y] = [t][z]$ is a trivial relation in G', that is $[x] = [t]$ and $[y] = [z]$, then from lemma 7.3 $x = t$ and $y = z$ in G and so $xy = tz$ holds trivially in G. So, Φ is an isomorphism of the groups G and G' and from lemma 7.5, G is Garside. □

7.2 Computation of Δ for a permutation solution

In this subsection, we consider the structure group of a non-degenerate, braided and involutive permutation solution. We claim that given the decomposition of the defining function of the permutation solution as the product of disjoint cycles, one can easily find a Garside element in its structure group. This result can be extended to non-degenerate and braided permutation solutions that are not involutive, using the construction from section 7.1.

Proposition 7.7. *Let $X = \{x_1, .., x_n\}$, and (X, S) be a non-degenerate, braided and involutive permutation solution defined by $S(i, j) = (f(j), f^{-1}(i))$, where f is a permutation on $\{1, .., n\}$. Let M be the monoid with the same presentation as the structure group. Assume that f can be described as the product of disjoint cycles:*
$f = (t_{1,1}, .., t_{1,m_1})(t_{2,1}, .., t_{2,m_2})(t_{k,1}, .., t_{k,m_k})(s_1)..(s_l)$, $t_{i,j}, s_* \in \{1, .., n\}$. *Then (i) For $1 \leq i \leq k$, $x_{t_{i,1}}^{m_i} = x_{t_{i,2}}^{m_i} = .. = x_{t_{i,m_i}}^{m_i}$ in M and this element is denoted by $x_{t_i}^{m_i}$.*
(ii) The element $\Delta = x_{t_1}^{m_1} x_{t_2}^{m_2} .. x_{t_k}^{m_k} x_{s_1} .. x_{s_l}$ is a Garside element in M.

We refer the reader to [2] for the proof.

References

[1] R. Charney, J. Meier and K. Whittlesey, Bestvina's normal form complex and the homology of Garside groups, Geometriae Dedicata *105* (2004) 171-188.

[2] F. Chouraqui, Decision problems in Tableau-groups and Tableau-semigroups, PhD thesis, Technion, Israel.

[3] A.H. Clifford, G.B. Preston, The algebraic theory of semigroups, vol.1, AMS Surveys *7*, (1961).

[4] P. Dehornoy, Groupes de Garside, Ann. Scient. Ec. Norm. Sup. *35* (2002) 267-306.

[5] P. Dehornoy, Braids and Self-Distributivity, Progress in Math. vol. 192, Birkhauser (2000).

[6] P. Dehornoy, Gaussian groups are torsion free, J. of Algebra *210* (1998) 291-297.

[7] P. Dehornoy, Complete positive group presentations, J. of Algebra *268* (2003) 156-197.

[8] P. Dehornoy, Y. Lafont, Homology of Gaussian groups, Ann. Inst. Fourier (Grenoble) *53-2* (2003) 489-540.

[9] P. Dehornoy, L. Paris, Gaussian groups and Garside groups, two generalizations of Artin groups, Proc. London Math. Soc. *79-3* (1999) 569-604.

[10] V.G. Drinfeld, On some unsolved problems in quantum group theory, Lec. Notes Math. *1510* (1992) 1-8.

[11] P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the Quantum Yang-Baxter equation, Duke Math. J. *100-2* (1999) 169-209.

[12] F.A. Garside, The braid group and other groups, Quart. J. Math. Oxford *20* No.78 (1969) 235-254.

[13] T. Gateva-Ivanova, A combinatorial approach to the set-theoric solutions of the Yang-Baxter equation, J. Math. Phys. *45-10* (2005) 3828-3858.

[14] T. Gateva-Ivanova, M. Van den Bergh, Semigroups of I-type, J. of Algebra *206-1* (1998) 97-112.

[15] E. Jespers, J. Okninski, Monoids and groups of I-type, Algebras and Representation Theory *8* (2005) 709-729.

[16] M. Picantin, The center of thin Gaussian groups, J. of Algebra *245* (2001) 92-122.

[17] M. Picantin, The conjugacy problem in Garside groups, Comm. in Algebra *29-3* (2001) 1021-1039.

[18] M. Picantin, Automatic structures for torus link groups, J. Knot Theory and its Ramifications *12-6* (2003) 833-866.

[19] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation, Advances in Math. *193* (2005) 40-55.